THAYER SCHOOL OF ENGINEERING AT DARTMOUTH

Information Markets for Security Experiments and Metrics

George Cybenko
Thayer School of Engineering
Dartmouth
gvc@dartmouth.edu

THAYER SCHOOL OF ENGINEERING AT DARTMOUTH

Security World Views Overview

	Formalism	World View	Examples
Ancient	Folklore/ Myths	Objects endowed with magical properties	MAC OS is "secure"; firewall + virus scanner means PC safe, etc
300 BC	Aristotelian	Objects, properties and relationships	Formal methods, expert systems, signature-based methods, etc
1700's	Newtonian/ Schrodingerian	System state and dynamics (stationary)	Control theory, Operations Research – deterministic and stochastic
1800's	Darwinian/ Smithian	Competition and constraints	Game theory, utility theory, pursuit and evasion
1900's	Kahnemanian	Human decision making and behaviors	"Law of Small Numbers", non-"optimal" behaviors

Each approach is "necessary but not sufficient"

THAYER SCHOOL OF ENGINEERING AT DARTMOUTH

What is an Information Market?

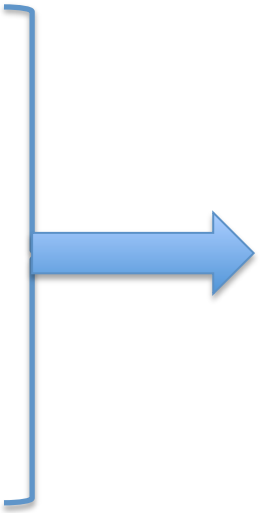
- "A speculative market created for the purpose of making predictions. The current market prices can then be interpreted as predictions of the probability of the event or the expected value of the parameter."
- "Also known as *prediction, decision, idea futures, event derivatives* or *virtual* markets."

(Wikipedia)

THAYER SCHOOL OF ENGINEERING AT DARTMOUTH

Role of Information Markets

- Formal/analytic inputs
- Experimental data
- Human insights



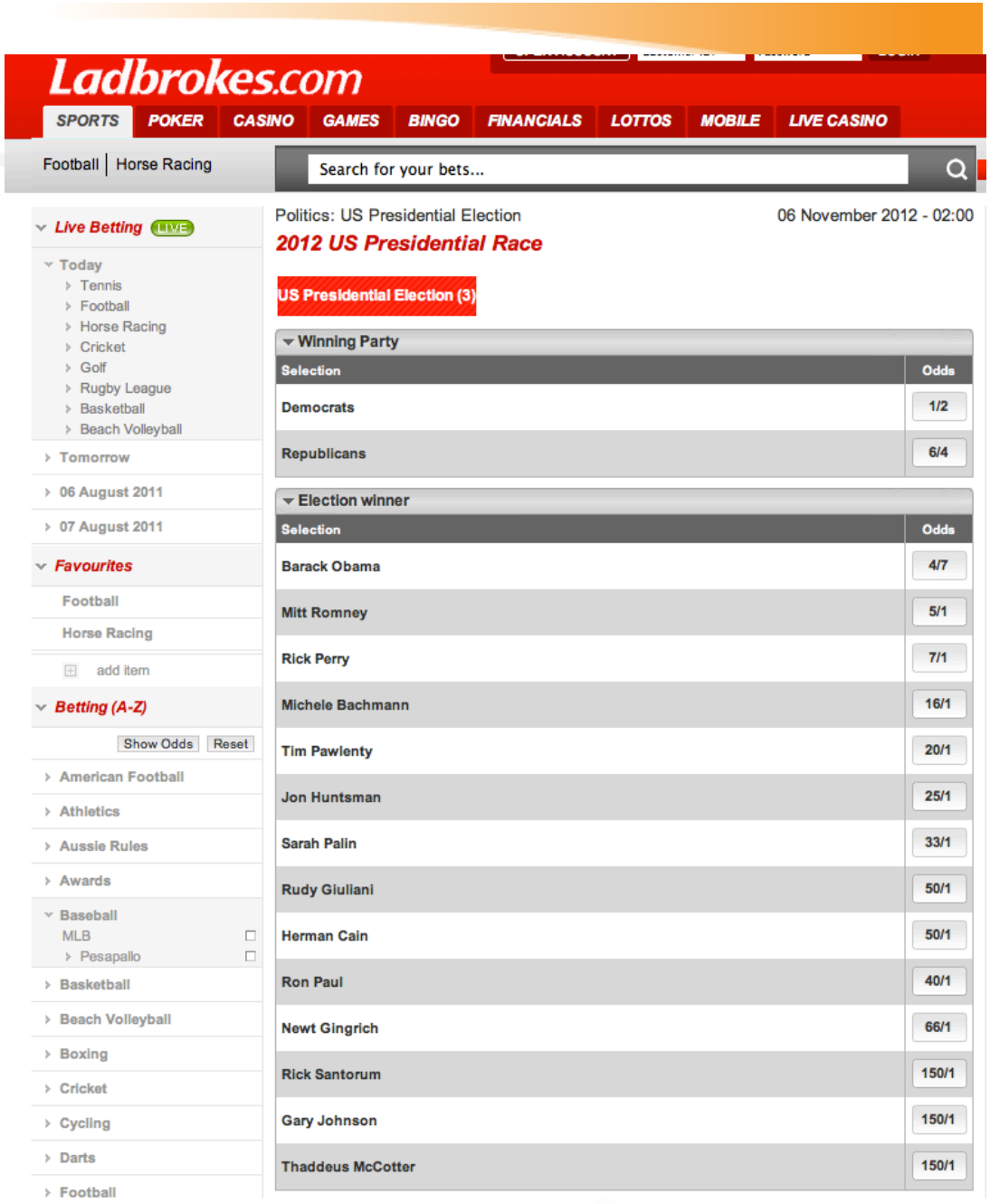
Combined through Information Markets

THAYER SCHOOL OF ENGINEERING AT DARTMOUTH

$$Odds = 1/2 = \frac{1 - p(A)}{p(A)}$$

Bet of \$2 wins \$1 if A happens

$$p(A) * winnings$$
$$-(1 - p(A)) * bet = 0$$



THAYER SCHOOL OF ENGINEERING AT DARTMOUTH

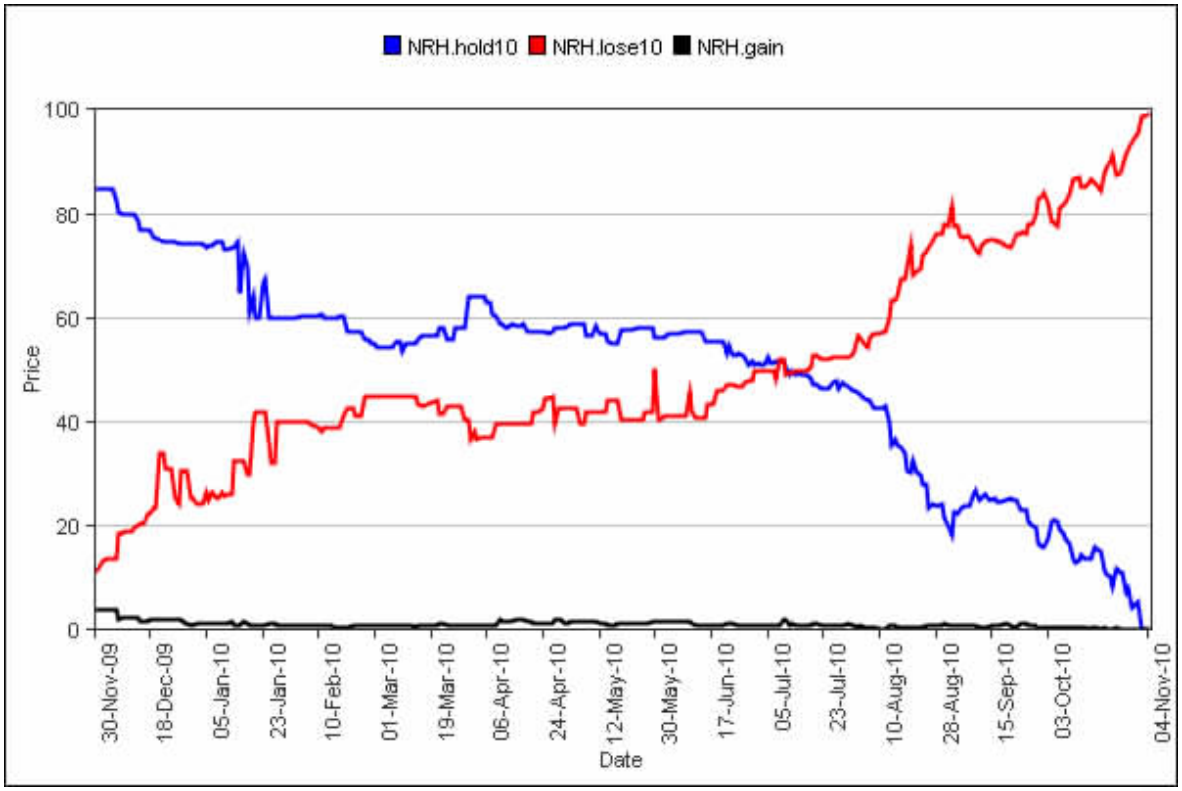
Polls vs Markets

- Poll – what will you do, what do you think, etc?
- Market – what do you think will happen, what will others do, etc?

Markets allow participants to integrate their insights with other's insights and are deemed more accurate for that reason.

THAYER SCHOOL OF ENGINEERING AT DARTMOUTH

Iowa Electronics Market (IEM)



Name	Description
NRH.gain10	$1 if the Democrats and Independents have more than 258 House seats; $0 otherwise
NRH.hold10	$1 if Democrats and Independents have more than 217 but no more than 258 House seats; $0 other
NRH.lose10	$1 if Democrats and Independents have 217 or fewer House seats; $0 otherwise

intrade BETA
The World's Leading Prediction Market

Search Markets e.g. Obama Go

Home | How it Works | Markets | Login | Sign Up

Home > Markets > Foreign Affairs/International Security > Middle East Protests > Muammar al-Gaddafi (Leader of Libya)

Muammar al-Gaddafi to no longer be leader of Libya before midnight ET 31 Dec 2011

Last prediction was: **$6.27** / share

Today's Change: ▼ **-$0.22** (-3.5%)

62.7%
CHANCE

Event: **Muammar al-Gaddafi (Leader of Libya)**

Advanced charts

Predict | View All Un-Matched Predictions | Info | Rules

Best (highest) price members are buying at

Price	Quantity
$6.10 / Share	2 shares
$6.09 / Share	4 shares
$5.60 / Share	15 shares
$5.54 / Share	2 shares
$5.23 / Share	3 shares
$5.10 / Share	5 shares
$5.00 / Share	8 shares
$4.90 / Share	5 shares
$4.80 / Share	5 shares
$4.70 / Share	5 shares
$4.60 / Share	5 shares
$3.32 / Share	1 share
$2.50 / Share	1 share
$0.08 / Share	50 shares
$0.01 / Share	6 shares

Best (lowest) price members are selling at

Price	Quantity
$6.48 / Share	5 shares
$6.49 / Share	5 shares
$6.50 / Share	13 shares
$6.55 / Share	12 shares
$6.57 / Share	3 shares
$6.58 / Share	9 shares
$6.59 / Share	100 shares
$6.69 / Share	4 shares
$6.70 / Share	1 share
$6.74 / Share	4 shares
$6.90 / Share	25 shares
$6.95 / Share	20 shares
$6.97 / Share	4 shares
$7.00 / Share	20 shares
$7.05 / Share	5 shares

THAYER SCHOOL OF ENGINEERING AT DARTMOUTH

Information Markets: NASDAQ Level II Order Book

Level2StockQuotes.com | NYSE Arca Book 1 | NYSE Arca Book 2

GET STOCK: YHOO go

Aggregate by Price

YHOO

LAST MATCH	
Price	16.7650
Time	10:31:51

TODAY'S ACTIVITY	
Orders	19,624
Volume	659,495

BUY ORDERS		SELL ORDERS	
SHARES	PRICE	SHARES	PRICE
10,065	16.7600	31,115	16.7700
10,407	16.7500	26,899	16.7800
16,559	16.7400	17,338	16.7900
20,996	16.7300	17,884	16.8000
23,578	16.7200	13,686	16.8100
9,660	16.7100	10,377	16.8200
12,365	16.7000	10,940	16.8300
7,767	16.6900	8,100	16.8400
19,592	16.6800	9,850	16.8500
1,600	16.6700	5,600	16.8600
7,600	16.6600	7,400	16.8700
29,200	16.6500	6,800	16.8800
1,700	16.6400	5,300	16.8900
600	16.6300	21,430	16.9000
600	16.6200	1,100	16.9100

THAYER SCHOOL OF ENGINEERING AT DARTMOUTH

Recent history of Information Markets for Security go back to an ill-fated DARPA Program in early 2000's

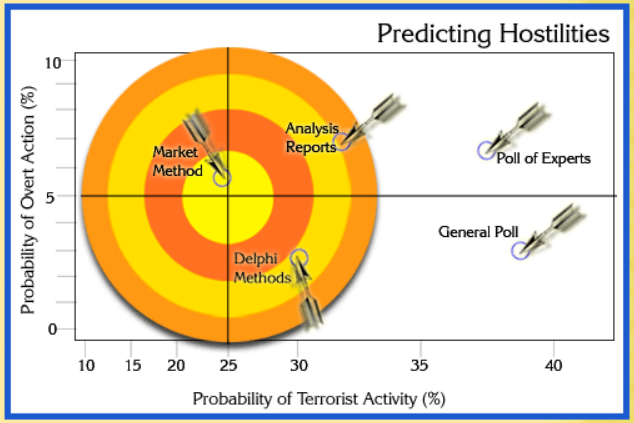
INFORMATION AWARENESS OFFICE

Scientia Est Potentia

Home | News | Programs | Solicitations

Return to Programs

FutureMap



Program Objective:

The DARPA FutureMAP (Futures Markets Applied to Prediction) program is a follow-up to a current DARPA SBIR, Electronic Market-Based Decision Support (SB012-012). FutureMAP will concentrate on market-based techniques for avoiding surprise and predicting future events. Strategic decisions depend upon the accurate assessment of the likelihood of future events. This analysis often requires independent contributions by experts in a wide variety of fields, with the resulting difficulty of combining the various opinions into one assessment. Market-based techniques provide a tool for producing these assessments.

There is potential for application of market-based methods to analyses of interest to the DoD. These may include analysis of political stability in regions of the world, prediction of the timing and impact on national security of emerging technologies, analysis of the outcomes of advanced technology programs, or other future events of interest to the DoD. In addition, the rapid reaction of markets to knowledge held by only a few participants may provide an early warning system to avoid surprise.

Program Strategy:

The DARPA FutureMAP program will identify the types of market-based mechanisms that are most suitable to aggregate information in the defense context, will develop information systems to manage the markets, and will measure the effectiveness of markets for several tasks. Open issues that will drive the types of market include information security and participant incentives. A market that addresses defense-related events may potentially aggregate information from both classified and unclassified sources. This poses the problem of extracting useful data from markets without compromising national security. Markets must also offer compensation that is ethically and legally satisfactory to all sectors involved, while remaining attractive enough to ensure full and continuous participation of individual parties. The markets must also be sufficiently robust to withstand manipulation. FutureMAP will bring together commercial, academic, and government performers to meet these challenges.

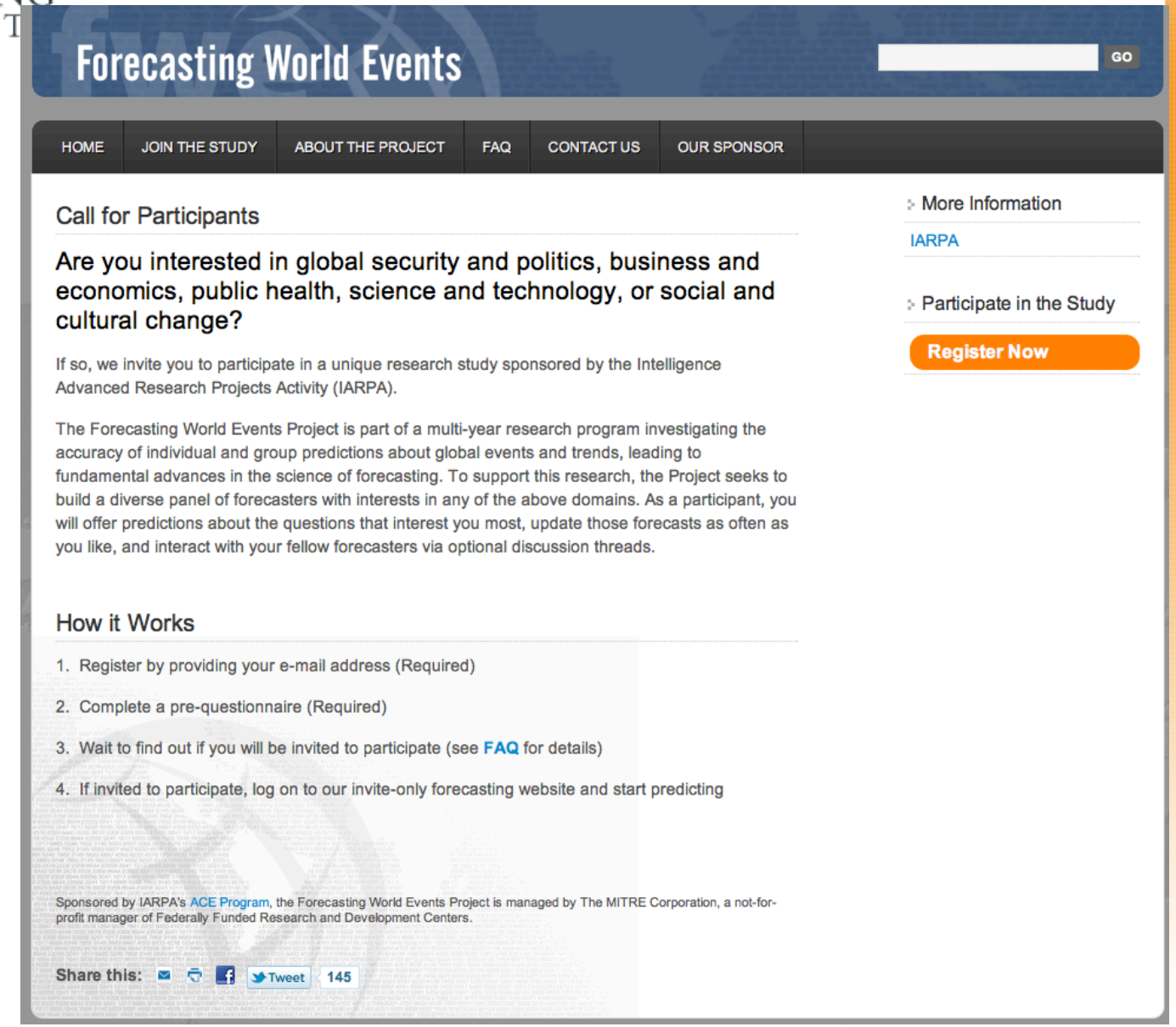
Planned Accomplishments:

TBD

Home News Programs Solicitations

THAYER SCHOOL OF ENGINEERING AT DARTMOUTH

But the concept is making a comeback…
IARPA Aggregative Contingent Estimation (ACE) Program



THAYER SCHOOL OF ENGINEERING AT DARTMOUTH

And being evaluated for simple Cyber Security questions (In-Q-Tel?)

CSDM
Cyber Security Decision Market

technology review
Published by MIT

Tuesday, July 5, 2011

A Futures Market for Computer Security

A predictions market could help companies prepare for major security incidents before they happen.
By Brian Krebs

Information security researchers from academia, industry, and the U.S. intelligence community are collaborating to build a pilot "prediction market" capable of anticipating major information security events before they occur.

A prediction market is similar to a regular stock exchange, except the "stocks" are simple statements that the exchange's members are encouraged to evaluate. Traders will buy and sell "shares" of a stock based on the strength of their confidence about the future outcome—with an overall goal of increasing the value of their portfolios, which will in turn earn them some sort of financial reward. Traders may choose to buy or sell additional shares of a stock, and that buying and selling activity pushes the stock price up or down, just as in a real market.

Some of the stocks being considering cover a few months, such as: "The volume of spam e-mail will increase by 10 percent in the third quarter of 2011." Others will ask participants to gauge the likelihood of far-off events, such as the chance that the U.S. House of Representatives will pass a bill with "cyber" and "security" in its title in the first session of the 112th Congress, or whether broadly used encryption algorithms will be defeated within the next 24 months.

Greg Shannon, chief scientist of the CERT program at Carnegie Mellon's Software Engineering Institute, who is involved with the project, says the purpose is to provide actionable data.

"If you're Verizon, and you're trying to pre-position resources, you might want to have some visibility over the horizon about the projected prevalence of mobile malware," Shannon said. "That's something they'd like to have an informed opinion about by leveraging the wisdom of the security community."

For Good Measure

New Measures

1. Your problem is not as unique as you think
2. You have more data than you think
3. You need less data than you think
4. There is a useful measurement that is much simpler than you think.

—Douglas W. Hubbard, *How to Measure Anything*

Regular readers of this column might recall the installment that appeared in the November/December 2010 issue, "An Index of Cybersecurity," which suggested that such an e ICS) would soon appear. Prophesy is now fulfilled: as begun publication at rityindex.org. It's what *sentiment-based index*— familiar with the US Confidence Index, already know what it /tinyurl.com/3sb633k). Respondents to the ICS are competent security practitioners with direct operational responsibility who share, each month, how their view of security in several areas has changed since the month before. Thanks to them for their willingness to engage.

The ICS will be published at 6:00 p.m. (Eastern time, US) on the last day of every month and available to all. My colleague Mukul Pareek and I are committed to making it a valuable and permanent resource. Those particularly interested in methodology might want to review the questions we ask and how we calculate the Index from the answers to those questions on the website.

Because it's well documented on the website, I won't give a more detailed explanation of the Index here. The "why" is straightforward: to communicate with each other, we need a structured, transparent, orderly mechanism for pooling what our most seasoned colleagues judge to be our current situation in cybersecurity. To communicate with others outside our field, we need to be boring, which is to say we need a communication medium that doesn't ask people outside our field to follow along as we break new methodological ground in survey research. We need a conventional index so that questions of form don't distract from the questions of whether the state space of cybersecurity is changing. We need something to cite.

The ICS is one leg of strategy; with colleagues Alex Hutton (Verizon) and Greg Shannon (CERT), the second leg is a formal prediction market for cybersecurity, now in beta test. Where the ICS is a measure of position, a prediction market is a measure of momentum (direction and velocity).[1] Prediction markets have an extensively documented theory and great design flexibility, but the short form description of the simplest prediction market is that in such a market the participants are vying with each other to better predict whether concrete future events will or will not occur. They do this by the buying and selling of contracts that posit that such and such an event will occur by such and such a time.[2]

Fact-seeking surveys, such as our ICS, are vulnerable to poor choices of respondents, so we control the survey population to avoid that problem. In contrast, fact-seeking markets, such as our Cyber Security Prediction Market (CSPM), are vulnerable to poor choices of questions. Taking as an axiom that the purpose of security metrics is decision support, per se, the kinds of questions to commit to the CSPM should be ones that provide maximally reliable decision support to the cybersecurity practitioner, are subject to expert disagreement, and yet are ultimately answerable. As you can imagine, this isn't so simple.

As a motivating example, consider the pressure on many enterprises to integrate the employee smartphone into the enterprise's information infrastructure. Besides the fact that this bulldozes the corporate perimeter, a planner might want to have a feel for whether over the next budget cycle the security problems of smartphones are likely to rise, likely to fall, or likely to lumber along at whatever level they now are. Such a decision aid can be readily formulated as one or more prediction

COPUBLISHED BY THE IEEE COMPUTER AND RELIABILITY SOCIETIES 1540-7993/11/$26.00 © 2011 IEEE MAY/JUNE 2011

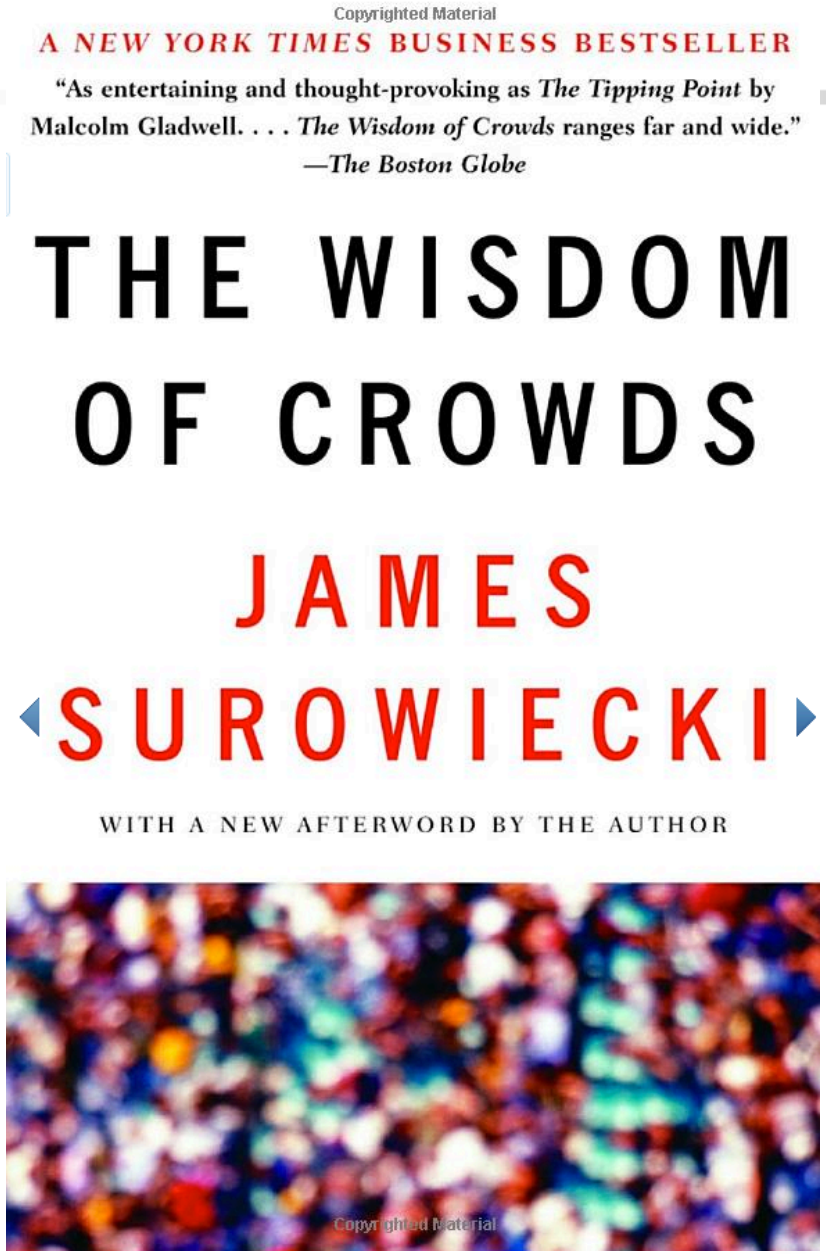
THAYER SCHOOL OF ENGINEERING AT DARTMOUTH

Sample CSDM Markets

Title, Contract Statement	Duration, Close Date	Decision Criteria, Data Sources
Out-of-order OS Patch Q3 2011 The market leader in U.S. commercial desktop operating systems issues an OS patch that is inconsistent with its announced patch release schedule.	One or more quarters End of quarter	Market leader: As reported by the latest reports from market analysts in the previous quarter. OS: The newest operating system sold by the vendor.
Spam Volume in May 2011 The volume of spam email will increase by 10% over April 2011.	One or more months End of month	Data: TBD, but roughly a widely cited source "selected" by the anti-spam community.
Regulation E in 2012 Regulation E will remain unchanged throughout 2012.	One or more years End of year	Unchanged: The text for Regulation E in the U.S. Code in effect in 2012 affecting regulation E will have no change. Data: Congressional Record
SHA-1 collision 2013 A valid SHA-1 collision is published in 2013.	One or more years End of year	Published: Details available to anonymous US users. Valid: Three tenured faculty in top-20 U.S. computer science departments positively confirm that "the collision is relevant to commercial reliance on SHA-1." Data: U.S. accessible Internet
House Cyber-Security Legislation 2011 The U.S. House will pass a bill with "cyber" and "security" in its title in the 1st session of the 112th Congress.	One or more years Typically December	Pass: Congressional Record reports the bill as passed within 10 government working days after the close of the session. Data: Congressional Record

THAYER SCHOOL OF ENGINEERING AT DARTMOUTH

Popularized in 2005

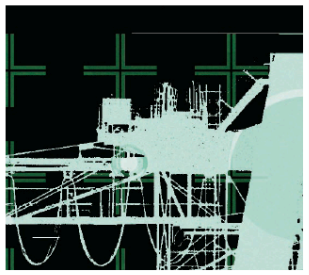


THAYER SCHOOL OF ENGINEERING AT DARTMOUTH

COMPUTING PRACTICES

Cybersecurity Strategies: The QuERIES Methodology

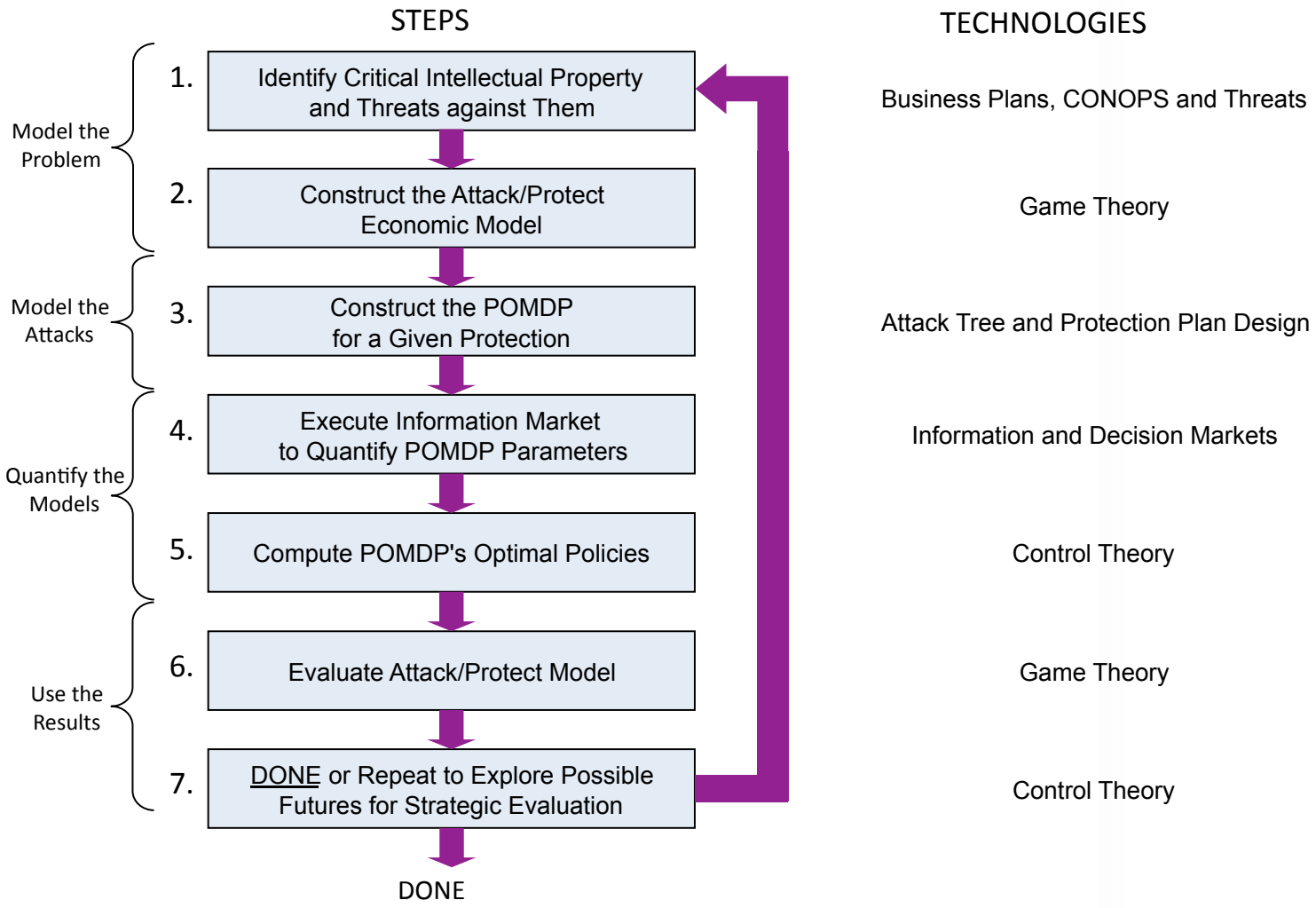
QuERIES offers a novel multidisciplinary approach to quantifying risk associated with security technologies resulting in investment-efficient cybersecurity strategies.



Carin, Cybenko and Hughes, IEEE Computer, August 2008

THAYER SCHOOL OF ENGINEERING AT DARTMOUTH

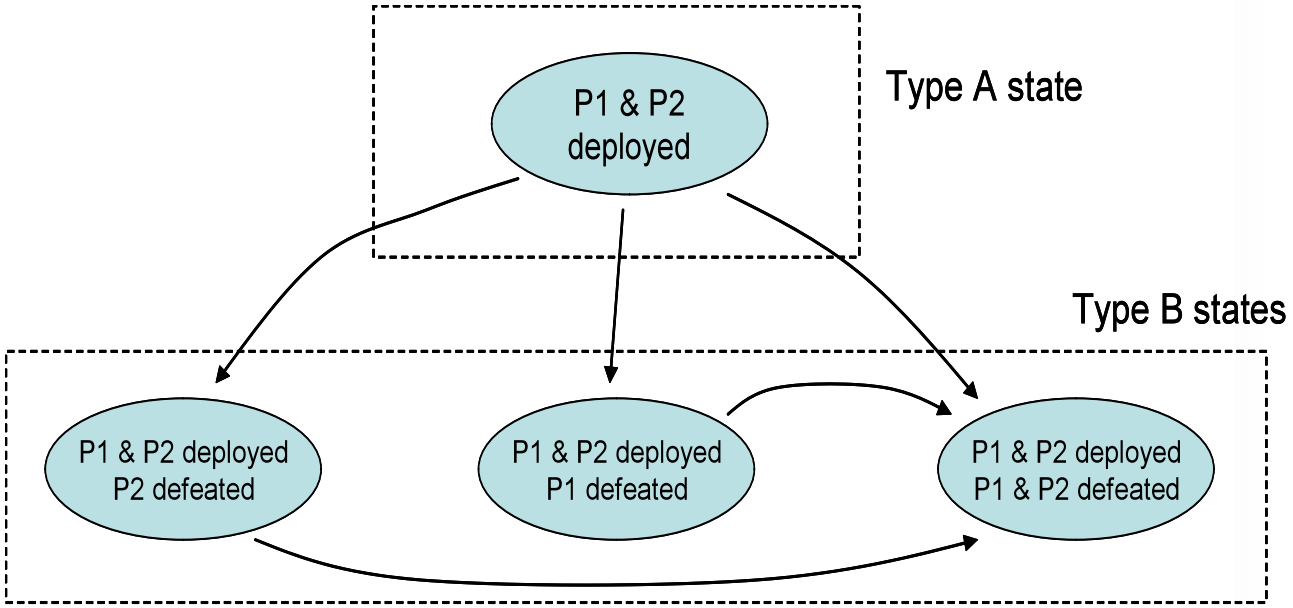
QuERIES Overview – 6 steps



Steps of the QuERIES Methodology

THAYER SCHOOL OF ENGINEERING AT DARTMOUTH

Markov Decision Process Modeling of an Attack



State of the attack are labeled by intact and defeated protections.

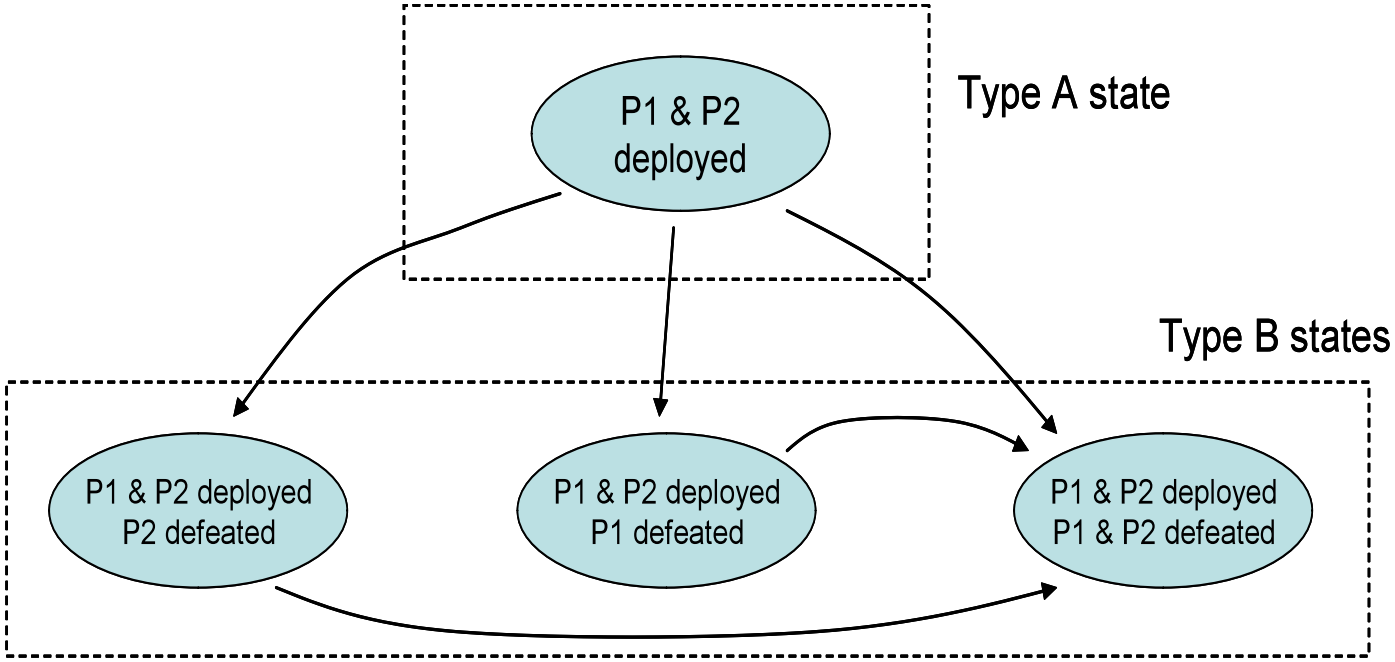
Attackers select actions which determine transition probabilities.

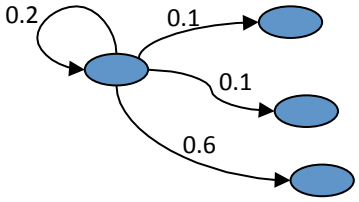
All transitions possible but not shown.

This is a Markov Decision Process (MDP).

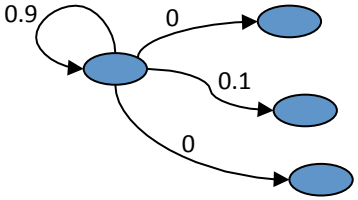
THAYER SCHOOL OF ENGINEERING AT DARTMOUTH

Markov Decision Process Modeling of an Attack

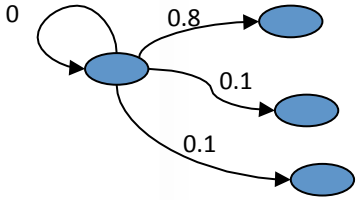




Transition probabilities for action "a"



Transition probabilities for action "b"

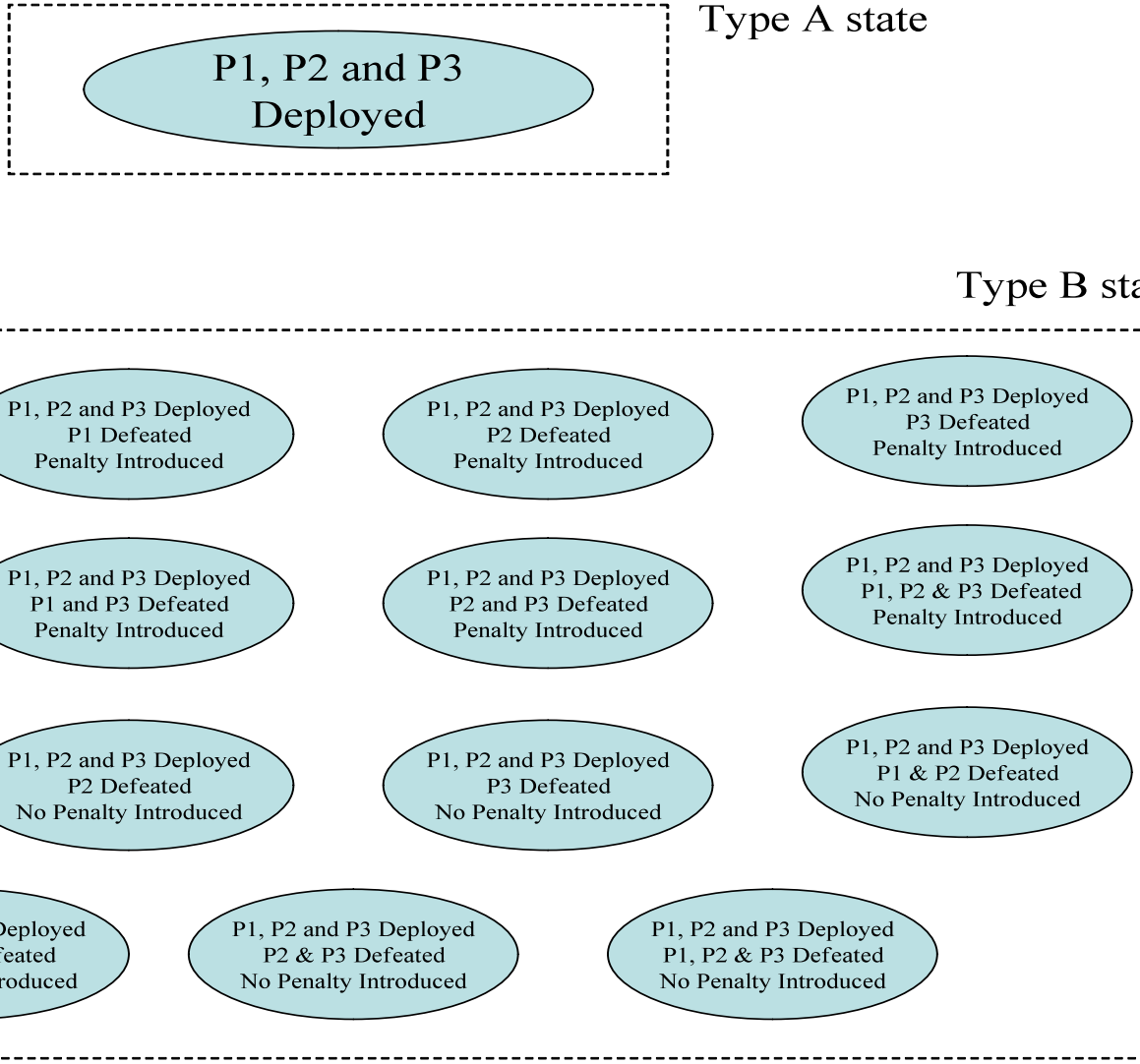


Transition probabilities for action "c"

Actions/state pairs have costs as well.

THAYER SCHOOL OF ENGINEERING AT DARTMOUTH

Markov Decision Process Modeling of an Attack: Scalability Issues

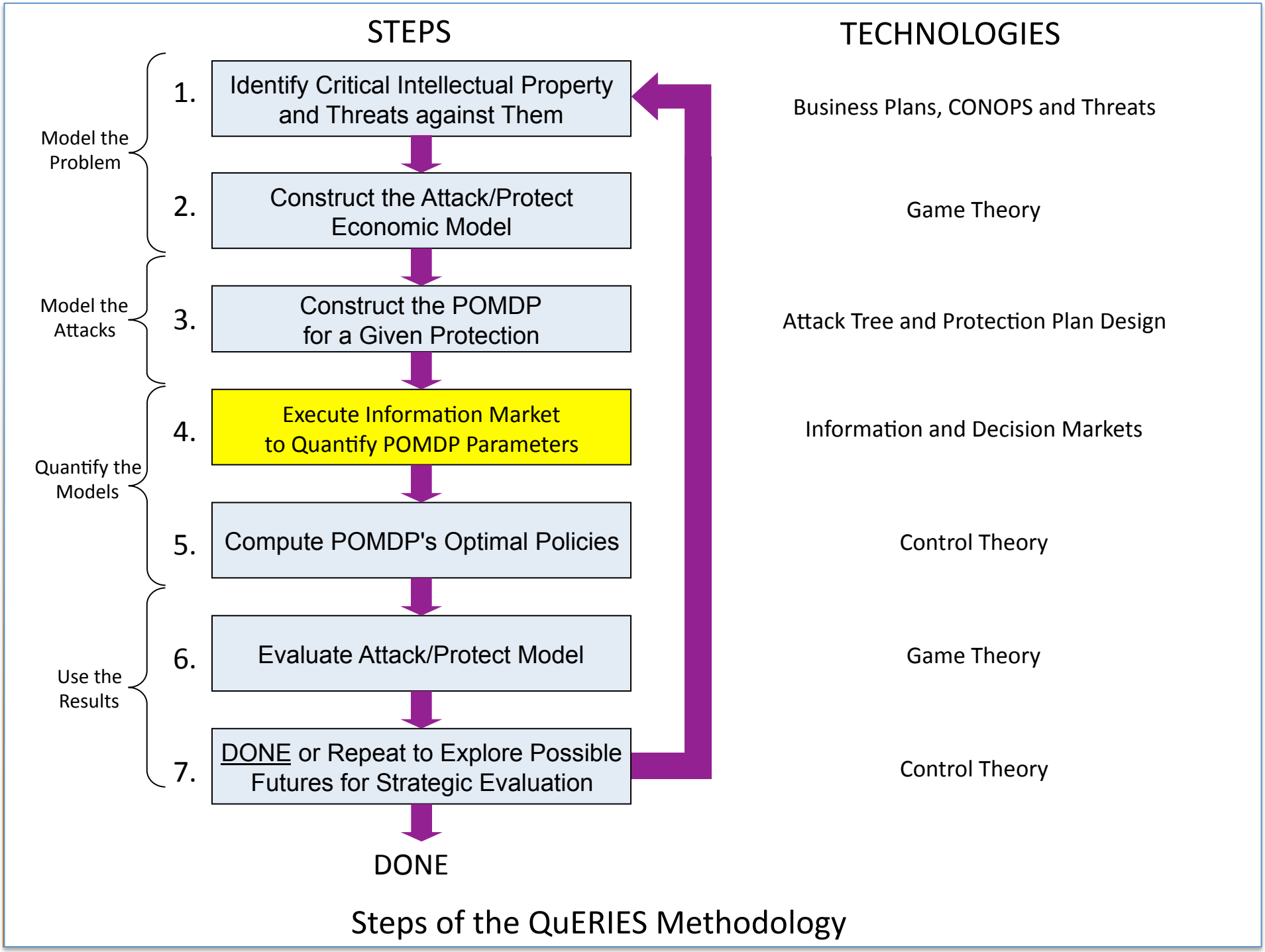


THAYER SCHOOL OF ENGINEERING AT DARTMOUTH

Two Important Aspects

1. There are many transition probabilities and costs to estimate:
   - Too many to obtain empirically using red teams

2. An attacker may not know which state they are in
   - This is a desirable feature of good protections!
   - Partially Observable MDP (POMDP) models
   - States are PDF's over attacker's beliefs



Steps of the QuERIES Methodology

THAYER SCHOOL OF ENGINEERING AT DARTMOUTH

Quantifying POMDP Parameters

Three Steps

1. Conduct a partial Red Team attack
2. Use Red Team participants in an information market to estimate POMDP parameters (using real money)
3. Use another Red Team or Whitehats to determine “truth” and subsequent payouts.

THAYER SCHOOL OF ENGINEERING AT DARTMOUTH

Partial Red Teaming Attack

- Independent attackers
- Given protected code but limited or no additional information
- They attempt a variety of attacks against code
- Partial because the goal is to learn about protections not to defeat them all
- Experienced Red Team members then participate in an information market

THAYER SCHOOL OF ENGINEERING AT DARTMOUTH

Information Markets

Technique for using groups of people to estimate probabilities or parameters

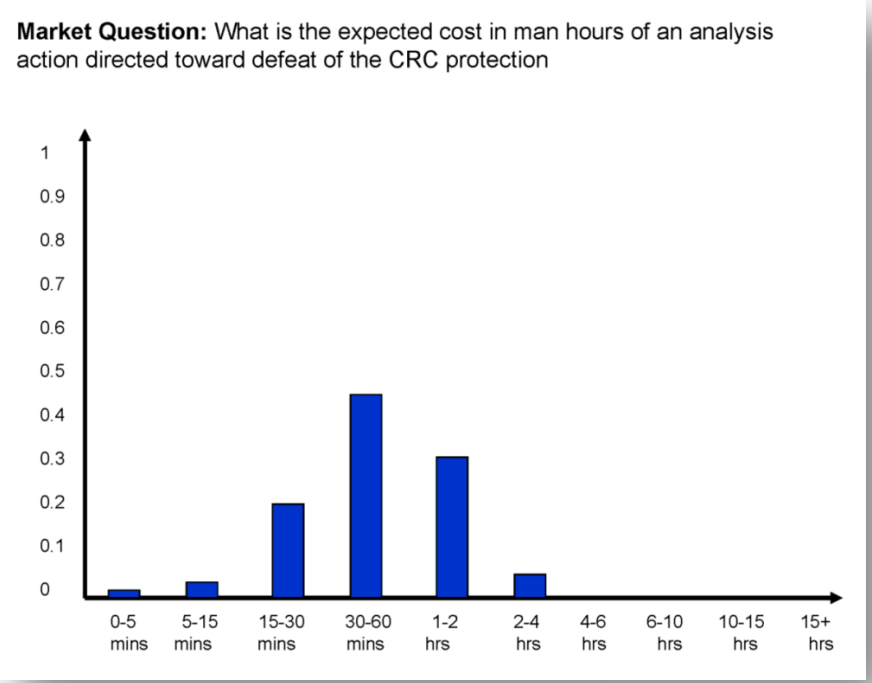
Examples:

- Parimutuel betting (probs)
- Iowa Electronic Markets (probs)
- Financial markets (means)
- Sports point spreads (median)

Works better if real money at stake

Polls – what will you do?
Markets – what will other people do?

See Market Scoring Rules, Robin Hanson, Information/Prediction/Decision Markets



We have used market scoring rules to estimate PDF's

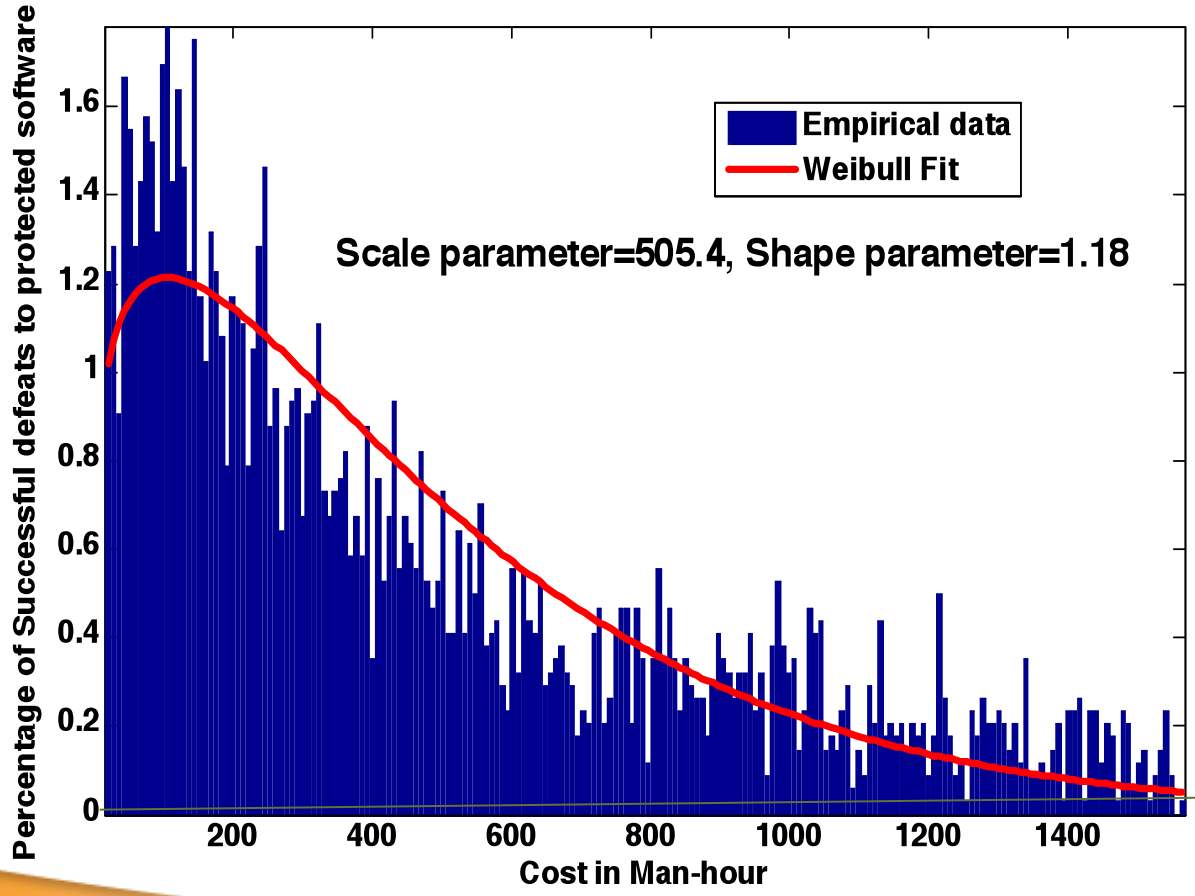
Solving POMDP's

- "Solving" a MDP or a POMDP means finding an optimal policy – ie. The assignment of actions to states that minimizes the specified cost
- This is a stochastic optimal control problem
- Solvable by dynamic programming techniques
- Scalability issues for POMDP's because of the size of the state space (technically infinite)
- Can find optimal action for each state, next best, third best, etc

THAYER SCHOOL OF ENGINEERING AT DARTMOUTH

Solving the POMDP

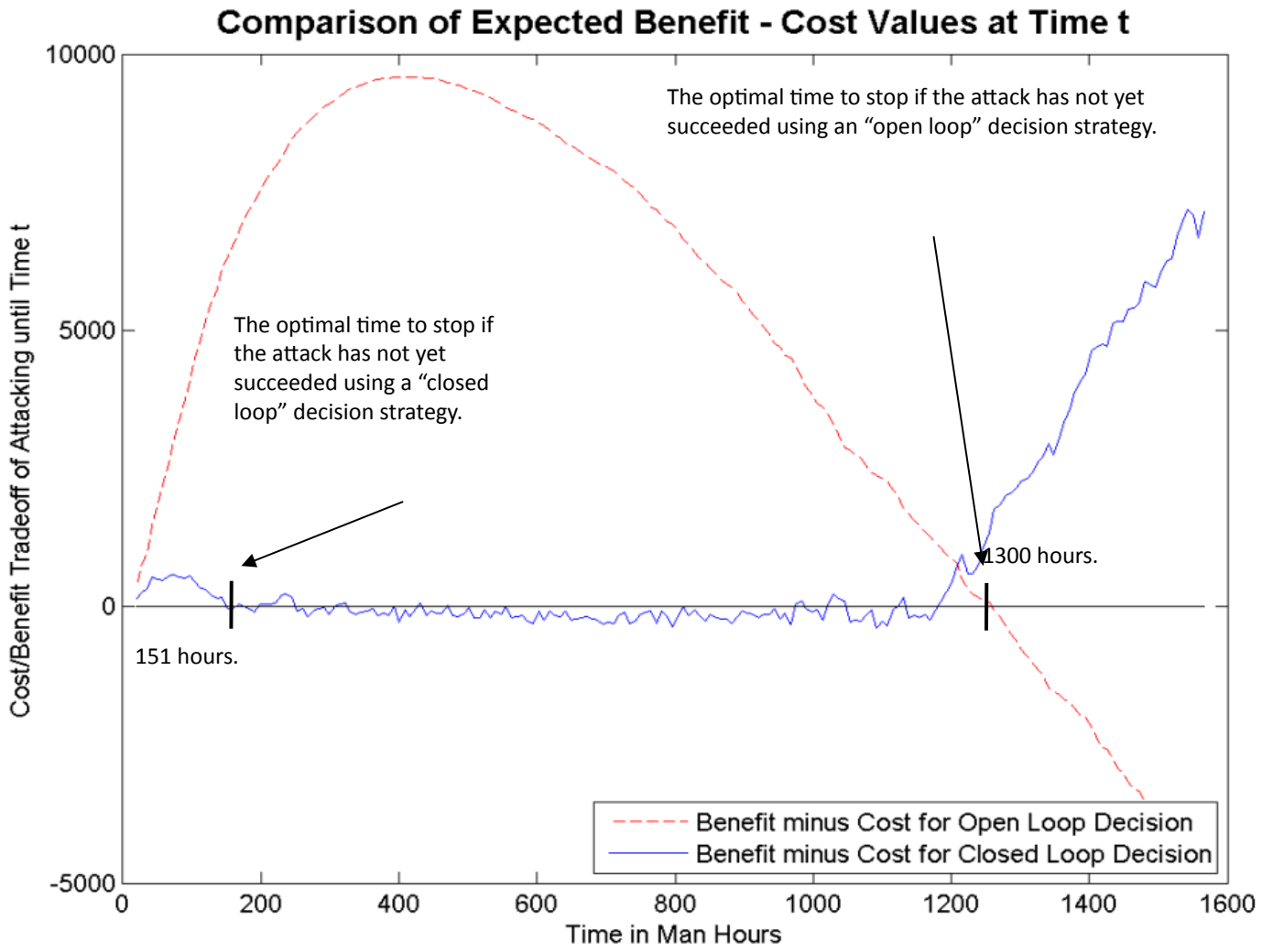
Generating Man-Hour (Cost) PDF's by Sampling from Policies – Expert (sample from optimal) to Novice (sample from k best policies) – Carin, Cybenko, Hughes – IEEE Computer 2008.



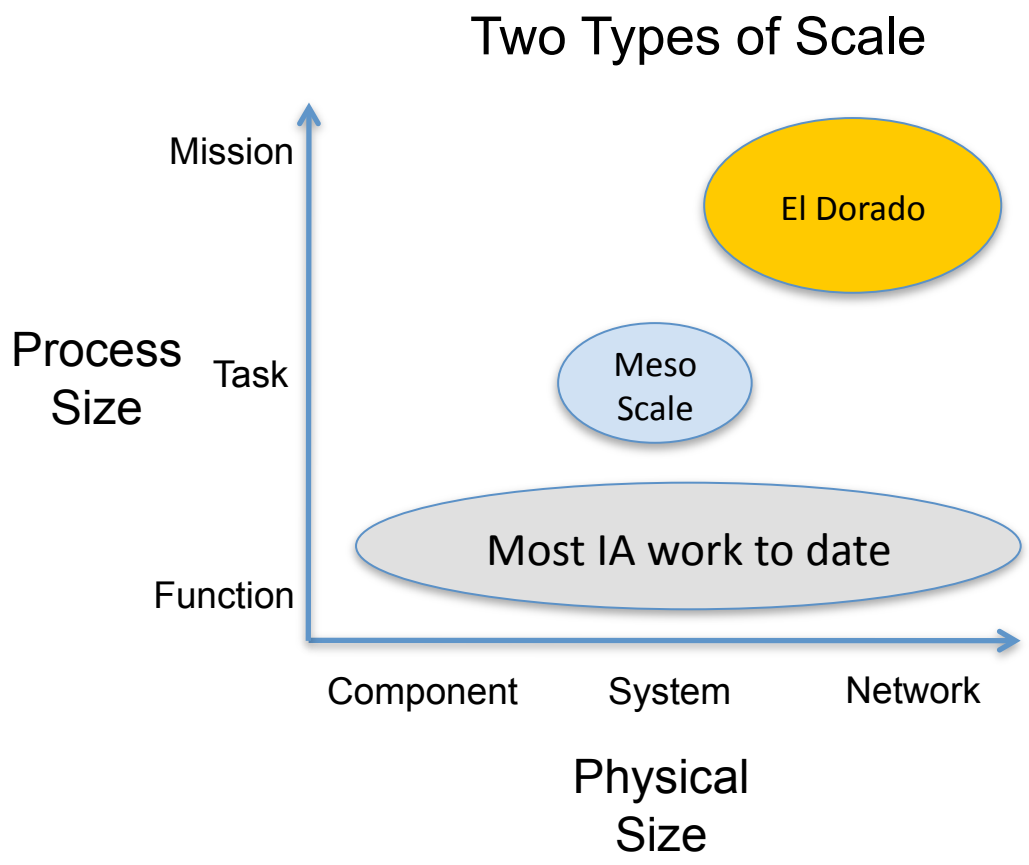
RSA, AES, etc

THAYER SCHOOL OF ENGINEERING AT DARTMOUTH

Then we could conclude things like…



Roadmap



Moving up in scale requires abstraction and information integration that we cannot do purely through formal methods and/or experiments.

Role of markets and compositional techniques (as in reliability theory) should be explored.

THAYER SCHOOL OF ENGINEERING AT DARTMOUTH

Summary

- Complex cyber systems = systems we cannot make formal, provable assertions about
- Complex cyber systems security properties are a combination of formal, experimental and human insights.
- Information markets in combination with experiments should be explored for cyber systems security properties